What is claimed:

1. A method for forming a strong password comprising the steps of:

obtaining biometric data from a user;

generating a one-time password for the user; and

combining the biometric data and the one-time password to form the strong password.

2. A method according to claim 1, further comprising the step of encrypting the combined one-time password and biometric data using an encryption key to form the strong password.

3. A method for controlling access to secure data comprising the steps of:

receiving a strong password including one-time password and biometric data from a user;

separating the one-time password and the biometric data;

comparing the one-time password to a calculated one-time password to determine if the one-time password is valid;

determining a probability that the biometric data is from the user;

encrypting the secure data using an encryption key to obtain encrypted data if the one-time password matches the calculated one-time password and the probability that the biometric data is from the user exceeds a predetermined threshold value;

combining the strong password, the encryption key and the encrypted data; and

transmitting the combined strong password, encryption key and encrypted data to the user.

4. A method according to claim 3, further including the step of encrypting the combined strong password and encryption key using a further encryption key.

5. A method according to claim 3, wherein the secure data includes items having respectively different security levels, and the step of encrypting the secure data aborts the method if either the one-time password does not match the calculated one-time password or the probability that the biometric data is from the user does not exceed the predetermined threshold value.

6. A system for implementing secure access to a remote computer system comprising:

at least one first computer securely coupled to the remote computer system;

at least one second computer coupled to said at least one first computer and configured to obtain identifying information from a user;

whereby the second computer passes the identifying information to the first computer, the first computer passes the identifying information to the remote computer system and the remote computer system verifies the identifying information.

7. A system according to claim 6, wherein the identifying information is a strong password including a one-time password and biometric information.

8. A system according to claim 7, wherein the identifying information is encrypted with an encryption key.

9. A system according to claim 8, wherein the at least one second computer is securely connected to said at least one first computer by means of a Secure Socket Layer connection.

10. A system according to claim 9, wherein the at least one second computer includes a further Secure Socket Layer connection for receiving the identifying information from the user.

11. A system according to claim 9, wherein the remote computer includes firewall software through which the at least one first computer is coupled to the remote computer.

12. A method of allowing access to secure data on a remote computer, including the steps of:

a) receiving a request from a user to access the secure data at a first computer;

b) transferring the request to access the secure data from the first computer to a second computer;

c) transferring the request to access the secure data from the second computer to the remote computer;

d) authorizing access to the secure data at the remote computer;

e) transferring the secure data to the second computer; and

f) transferring the secure data from the second computer to the user without using the first computer.

13. A method according to claim 12, wherein the request to access the secure data includes a strong password and step e) includes the steps of:

encrypting the secure data with an encryption key;

combining the encryption key with the strong password;

encrypting the combined encryption key and strong password with a further encryption key; and

transferring the encrypted combined encryption key and strong password and the encrypted secure data to the second computer.

14. A method according to claim 13 wherein the step of encrypting the data with an encryption key includes encrypting the data with a symmetric encryption key and the step of encrypting the combined encryption key and strong password with a further encryption key includes the step of encrypting the combined encryption key and strong password with an asymmetric encryption key.

15. A method according to claim 14, wherein the strong password includes a one-time password and biometric information and the step d) includes the steps of:

separating the one-time password and the biometric information;

comparing the one-time password to a calculated one-time password;

determining a probability that the biometric information matches an authorized user; and

authorizing access to the secure data only if the one time password matches the calculated one-time password and the probability that the biometric information matches an authorized user exceeds a predetermined threshold value.

16. A computer readable carrier including computer program instructions that cause a computer to form a strong password comprising the steps of:

obtaining biometric data from a user;

generating a one-time password for the user; and

combining the biometric data and the one-time password to form the strong password.

17. A computer readable carrier according to claim 16, wherein the computer program instructions further cause the computer to perform the step of encrypting the combined one-time password and biometric data using an encryption key to form the strong password.

18. A computer readable carrier including computer program instructions that cause a computer to implement a method for controlling access to secure data comprising the steps of:

receiving a strong password including one-time password and biometric data from a user;

separating the one-time password and the biometric data;

comparing the one-time password to a calculated one-time password to determine if the one-time password is valid;

determining a probability that the biometric data is from the user;

encrypting the secure data using an encryption key to obtain encrypted data if the one-time password matches the calculated one-time password and the probability that the biometric data is from the user exceeds a predetermined threshold value;

combining the strong password, the encryption key and the encrypted data; and

transmitting the combined strong password, encryption key and encrypted data to the user.

19. A computer readable carrier according to claim 18, wherein the computer program instructions further cause the computer to perform the step of encrypting the combined strong password and encryption key using a further encryption key.

20. A computer readable carrier according to claim 19, wherein the secure data includes items having respectively different security levels, and the computer program instructions further cause the computer to perform the step of aborting the method if either the one-time password does not match the calculated one-time password or the probability that the biometric data is from the user does not exceed the predetermined threshold value.